UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, Plaintiff, v. MAXIM SENAKH, a/k/a "Mikhail Katsap," a/k/a "Andrey Rasputnikov," a/k/a "Stepan Demidov," Defendant.	)	**INDICTMENT** CR15-11 PJS/JSM 18 U.S.C. § 2 18 U.S.C. § 371 18 U.S.C. § 1030 18 U.S.C. § 1343

THE UNITED STATES GRAND JURY CHARGES THAT:

1. Beginning in 2011 and continuing to the present day, the defendant, MAXIM SENAKH, and his co-conspirators hacked into and installed malicious computer software on thousands of computer servers located in Minnesota and throughout the world ("compromised computer servers"). This malicious software enabled the defendant and his co-conspirators to gain covert access to and control over the compromised computer servers. These servers could then be used by members of the conspiracy for illegal purposes, without the owners' knowledge or authorization. Since 2011 the defendant and his co-conspirators have used this network of compromised servers to send millions of Spam e-mail messages and to engage in advertising fraud. The defendant and his co-conspirators have obtained millions of dollars as a result of this criminal scheme.

Background

At all times relevant to this Indictment, unless otherwise stated:

2. "Pay-per-click" advertising is a common, legitimate form of web advertising. Pay-per-click advertisements are commonly found on the websites of newspapers and other media websites (these websites will be referred to below as "Host Websites"). When a visitor to such a Host Website clicks on the pay-per-click advertisement, the visitor is automatically taken to the advertiser's site. Advertisers generally utilize "affiliates" to find Host Websites for their advertisements. The affiliate provides a service to the advertiser, namely, finding Host Websites willing to host the advertiser's pay-per-click advertisement. The affiliate receives a commission for this service based upon the number of visitors to the Host Website who actually click on the pay-per-click advertisement. The Host Website receives a portion of the commission to compensate it for its willingness to host the pay-per-click advertisement.

3. The purpose of the scheme alleged herein was to fraudulently increase the commissions paid to defendant and his co-conspirators by redirecting visitors from other websites to the websites of advertisers in a manner designed to look like the visitor clicked a pay-per-click advertisement. The scheme also was designed to inflate the amount of Internet traffic to advertisers' websites by sending out millions of Spam e-mail messages with links that were enticingly and misleadingly mislabeled.

4. Defendant MAXIM SENAKH, also known as "Mikhail Katsap," "Andrey Rasputnikov," and "Stepan Demidov," was a Russian citizen residing in Russia.

5. Adult Friend Finder ("AFF") was an Internet-based adult dating and social networking service owned by FriendFinder Networks, a company based in Florida. AFF hired the defendant to act as an affiliate and direct traffic to AFF websites.

6. The Infinity Network ("Infinity") was a website marketing and development company operating from Los Angeles, California that acted as an affiliate. Advertisers hired Infinity to direct visitors to their websites in exchange for payment. Advertisers paid Infinity based on the number of visitors Infinity directed to their websites. Infinity hired the defendant to assist it in directing Internet traffic to advertisers that had hired Infinity.

7. Payoneer was a web-based payment processing and money transfer service based in the state of New York.

8. Paxum was a web-based payment processing and money transfer service based in Quebec, Canada.

The Defendant's Scheme

9. The defendant and his co-conspirators hacked into thousands of computer servers and installed a kind of malicious software, sometimes referred to as "malware," known as "Ebury." A "server" is a centralized computer with extra processing power that provides resources for and interacts with hundreds or thousands of other computers connected to it via a network, such as the Internet. Servers can be used to provide a variety of services, including hosting websites (a "web server"), routing e-mail (a "mail server"), or providing a centralized storage location.

10. Once installed, the Ebury Malware was used to surreptitiously steal log-on credentials (e.g., usernames and passwords) for the compromised server. Stealing the log-on credentials allowed the defendant and his co-conspirators to obtain "backdoor" access to and control over the computer servers, that is, covert, unauthorized access and control. The Ebury Malware also allowed the defendant and his co-conspirators to steal log-on credentials for any computer server that connected to compromised computer servers, thereby allowing the defendant and his co-conspirators access to and control over these servers as well.

11. Once the Ebury Malware was installed on a computer server, the computer server could be controlled remotely by the defendant and his co-conspirators. A computer server infected with malware that allows it to be controlled remotely, without the owner's knowledge or authorization, is referred to as a "bot," and collectively, the network of infected computer servers is referred to as a "botnet." The botnet infected with the Ebury Malware is referred to as the Ebury Botnet. The defendant and his co-conspirators used their unauthorized access to install other malware and run programs on the bots without the owners' knowledge or authorization.

12. The defendant and others used one or more of the infected computer servers as a "command-and-control" server. A "command-and-control" server is a centralized server that the other bots report to and provide information to, and can be used to control the other computer servers that make up the botnet. To avoid detection, the defendant and others changed command-and-control servers periodically throughout the conspiracy.

13. From in or about 2011, to the date of this Indictment, the defendant conspired with others to deploy the Ebury Botnet, which they used to generate revenue by engaging in click-fraud and redirecting web traffic through mass Spam e-mailing.

14. The click-fraud was accomplished by the defendant and his co-conspirators by installing additional malware on Ebury-infected computer servers. When users visited websites that were hosted on Ebury-infected computer servers, the malware automatically directed them from the website, through the Ebury Botnet, and to an advertiser's website. The advertiser's website to which the individuals were redirected had hired the defendant as an affiliate. The redirection was programmed so as to make it appear that the redirected web traffic came from a user who had "clicked" on an advertisement placed by the defendant for that advertiser when in fact nobody had clicked on any advertisement and users were instead redirected unwittingly from another website.

15. The defendant and his co-conspirators also used the Ebury Botnet to send hundreds of thousands of Spam e-mail messages. "Spam" e-mail messages are unsolicited bulk commercial e-mail messages. The content of these Spam e-mail messages was designed to entice users to click on links contained in the messages. When Spam recipients clicked on the link, they would be routed by an Ebury-infected computer server to the websites of advertisers for which defendant was an affiliate.

16. To conceal his identity and the nature of the fraudulent scheme, the defendant utilized multiple aliases and fraudulent identification documents; registered and used multiple e-mail addresses; leased and operated multiple servers, including servers designed to hide his identity called "proxy servers"; registered and operated

multiple domain names; created corporate entities for the purpose of receiving payments; and opened and transmitted funds through multiple web-based payment accounts and bank accounts.

COUNT 1

(Conspiracy to Violate the Computer Fraud and Abuse Act, and to Commit Wire Fraud, 18 U.S.C. §§ 371; 1030(a)(2)(C), (a)(4), (a)(5)(A); 1343)

17. The allegations contained in paragraphs 1- 16 of this Indictment are realleged and incorporated by reference as if fully set forth herein.

18. From at least in or about 2011 and continuing through the date of this Indictment, in the District of Minnesota and elsewhere, the defendant,

MAXIM SENAKH,
a/k/a "Mikhail Katsap,"
a/k/a "Andrey Rasputnikov,"
a/k/a "Stepan Demidov,"

did willfully and knowingly conspire, combine, confederate, and agree, together and with others both known and unknown to the Grand Jury, to commit offenses against the United States, that is:

a. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, thus causing damage affecting ten or more protected computers during a one-year period, and causing loss aggregating at least $5,000 in value to one or more persons during any one-year period from a related course of

conduct affecting one or more other protected computers, all in violation of 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(A)(i)(I) & (VI), and (c)(4)(B);

b. to knowingly and with intent to defraud, access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, to wit: revenue from a scheme to defraud advertisers, all in violation of 18 U.S.C. § 1030(a)(4) and (c)(3)(A);

c. to intentionally access a computer without authorization, and exceed authorized access, and thereby obtain information from a protected computer (namely, usernames and passwords), for purposes of commercial advantage and private financial gain, and in furtherance of any criminal and tortious act in violation of the Constitution and laws of the United States or of any state, all in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(i)–(ii); and,

d. to devise a scheme and artifice to defraud Internet advertisers, and to obtain money and property (namely, revenue from advertisers), by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of 18 U.S.C. § 1343.

Purpose of the Conspiracy

19. The purpose of the conspiracy was to generate revenue by using the Ebury Botnet to engage in click-fraud and to send Spam e-mail messages intended to redirect traffic to advertiser websites for which the defendant acted as an affiliate.

Manner and Means of the Conspiracy

20. It was part of the conspiracy that the defendant established advertising affiliate relationships directly with advertisers, including AFF, and indirectly through other affiliates, including Infinity. As an affiliate, the defendant received compensation based on the amount of Internet traffic that the defendant directed to an advertiser's website, in part measured through "clicks" on advertisements or links in Spam e-mail messages.

21. It was further part of the conspiracy that the defendant obtained from AFF various identifiers, including but not limited to a "Global Personal Identifier" (the "GPID") and a "Personal Identifier" (the "PID"), which he could electronically embed in AFF advertisements he placed. The GPID and PID were used to track the number of advertisements placed by the defendant and to calculate the amount of money to be paid to the defendant for clicks attributed to these advertisements.

22. It was further part of the conspiracy that Infinity assigned the defendant multiple "Promo Codes," which the defendant could electronically embed in advertisements he placed. Like the GPID and the PID, the Promo Codes were used to track Internet traffic directed by the defendant to specific websites, for which he was an Infinity affiliate and to calculate the corresponding payment to be made to the defendant.

23. It was further part of the conspiracy that the defendant and others surreptitiously installed Ebury Malware on thousands of computer servers and stole the compromised servers' log-on credentials, without the owners' knowledge or authorization.

24. It was further part of the conspiracy that the defendant and others caused Ebury Malware to covertly transmit the stolen log-on credentials to Ebury Botnet command-and-control servers, without the owners' knowledge or authorization.

25. It was further part of the conspiracy that the defendant configured one or more of the Ebury-infected computer servers to direct users who clicked on links in Spam e-mail messages to websites for which the defendant was hired as an affiliate.

26. It was further part of the conspiracy that each server infected with Ebury Malware became part of the Ebury Botnet.

27. It was further part of the conspiracy that the defendant and others used their "backdoor" access to the bots to surreptitiously install and operate additional malware or other files, without the owners' knowledge or authorization. For example, the defendant and others installed additional malware and files, which were used to transmit Spam e-mail messages through the Ebury Botnet; to re-direct Internet traffic through the Ebury Botnet; and to create new command-and-control servers.

28. It was further part of the conspiracy that the defendant used fictitious names, false contact information, and fraudulent identification documents to lease and operate proxy servers for the Ebury Botnet and to register Ebury command-and-control domains.

29. It was further part of the conspiracy that the defendant and others installed custom-designed malware on Ebury-infected servers. The malware caused visitors to websites hosted on Ebury-infected servers to be redirected through the Ebury Botnet to specified advertiser websites, while fraudulently giving the appearance that the visitor had clicked on an advertisement placed by the defendant, thus resulting in the generation of revenue for the defendant.

30. It was further part of the conspiracy that the defendant and others caused the daily transmission of hundreds of thousands of Spam e-mail messages through the Ebury Botnet to e-mail accounts around the world. Recipients of Spam e-mail messages who clicked on links contained in the Spam e-mail message would be directed by the Ebury Botnet to an advertiser's website, in order to generate revenue for the defendant.

31. It was further part of the conspiracy that the defendant and others, as advertising affiliates, received millions of dollars as a result of their click-fraud and Spam scheme, all while concealing the true nature and source of their operations.

32. It was further part of the conspiracy that the defendant and others caused log-on credentials, malware, and Spam e-mail messages to be transmitted over the Internet, such that they were transmitted in interstate commerce by means of wire communications.

Overt Acts of the Conspiracy

33. In furtherance of the conspiracy, and for the purpose of bringing about its unlawful objectives, the defendants and others committed and caused to be committed

overt acts in the District of Minnesota and elsewhere, including the following acts, among others:

Laying the Groundwork

34. On or before February 18, 2011, using the alias "Mikhail Katsap" and the e-mail address "Katsepsacc@gmail.com," the defendant became an advertising affiliate for AFF, with the intent of using this position to fraudulently obtain payments from AFF. AFF assigned defendant the GPID "g242405" and the PID "p1011105," which he could electronically embed in AFF advertisements that he distributed for tracking and payment purposes.

35. On or before July 21, 2011, using the alias "SF" and the e-mail address "silver777fox@gmail.com," the defendant became an advertising affiliate for Infinity, with the intent of using this position to fraudulently obtain payments from advertisers. Infinity assigned the defendant multiple "Promo Codes" that he could electronically embed in advertising that he distributed for tracking and payment purposes.

36. On or before October 15, 2010, the defendant opened a Payoneer account under his true identity, using the e-mail address "aff766817@gmail.com."

37. On or before December 7, 2010, the defendant opened a separate Payoneer account under the alias "Mikhail Katsap," using the e-mail address "Katsepsacc@gmail.com."

38. On or before September 29, 2011, the defendant opened a Paxum account using the alias "Stepan Demidov" and e-mail address "demidov70s@gmail.com."

39. On or before February 9, 2012, using the alias "Mikhail Katsap," the defendant created the corporate entity "Germes Management, Ltd."

40. On or about March 1, 2013, the defendant registered one or more Ebury Botnet command-and-control domains, including the domain "o8rad5ccx9f3r.net," under the alias "Andrey Rasputnikov" and the e-mail address "rasputnig@googlemail.com."

41. On or about July 11, 2013, the defendant used a server located in South Africa (the "South African Server") as an Ebury Botnet command-and-control server. On or about July 11, 2013, the defendant assigned the domain "o8rad5ccx9f3r.net" to the South African Server.

Accessing and Infecting Servers with Ebury Malware

42. On or about the following dates, one or more members of the conspiracy caused Ebury Malware to be installed on the following computer servers, without the owner's knowledge or authorization:

a. On or before August 26, 2013, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server located in Minneapolis, Minnesota, and belonging to "G.L." (the "Minneapolis Server").

b. On or before September 11, 2013, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server located in Duluth, Minnesota, and belonging to SuperiorUSA Corp., a Minnesota company (the "Duluth Server").

c. On or before August 8, 2013, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server belonging to Nagem Medical Specialties, LLC (the "Nagem Server").

d. On or before October 16, 2013, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server located in Turkey (the "Turkish Server").

e. On or before October 16, 2013, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server located in the Netherlands (the "Dutch Server").

f. On or before February 27, 2014, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server hosting the Thai-language website "dek-zaa.com."

g. On or before January 15, 2014, one or more members of the conspiracy caused Ebury Malware to be installed on a computer server hosting the websites "photographersupplystation.com" and "myphotohome.com."

43. On or about the following dates, one or more members of the conspiracy caused Ebury Malware to covertly steal and transmit log-on credentials to a bot under their control, without the owner's knowledge or authorization:

a. On or before August 26, 2013, one or more members of the conspiracy caused Ebury Malware to steal log-on credentials for the Minneapolis Server and transmit them to the South African Server.

b. On or before September 11, 2013, one or more members of the conspiracy caused Ebury Malware to steal log-on credentials for the Duluth Server and transmit them to the South African Server.

Using the Ebury Botnet to Redirect Internet Traffic and Engage in Click-Fraud

44. On or about February 27, 2014, using custom-designed malware, the defendant and others caused one or more visitors to the Thai-language website "dek-zaa.com," to be unwittingly and automatically re-directed through the Turkish and Dutch Servers to an AFF website, while using the defendant's assigned GPID and PID to make it appear to AFF that the visitors had "clicked" on an AFF advertisement placed by the defendant.

45. On or about January 15, 2014, the defendant caused one or more visitors to the websites "photographersupplystation.com" and "myphotohome.com," to be unwittingly and automatically redirected through the Ebury Botnet to an AFF website, while using the defendant's assigned GPID and PID to make it appear to AFF that the visitors had "clicked" on an AFF advertisement placed by the defendant.

Using the Ebury Botnet to Send Spam E-mail Messages and Direct Internet Traffic

46. On or about July 7, 2011, the defendant, using an alias, registered the domain name "susie-hiniker.info."

47. On or about July 13, 2011, the defendant caused Spam e-mail messages to be sent, where the sender of the e-mail was falsely identified as "susie_hiniker@susie-hiniker.info," and the e-mail contained the text, "I'm back in town. Remember me?" and

a hyperlink to "http://www.susie-hiniker.info/." The defendant intended the recipients of the e-mail to click on the link to "www.susie-hiniker.info."

48. On or about May 5, 2012, the defendant, using an alias, registered the domain name "breanna-mcghee.in."

49. On or about May 9, 2012, the defendant caused Spam e-mail messages to be sent, where the sender of the e-mail was falsely identified as "breanna_mcghee@breanna-mcghee.in," and the e-mail contained an image along with the text:

> I created a profile at this site: http://www.breanna-mcghee.in
> You can get my phone number there if you want to go on a date with me.
> Make sure you rent a room at a nice hotel with a queen size bed!

The defendant intended the recipients of the e-mail to click on the link "www.breanna-mcghee.in."

50. On or before October 31, 2013, the defendant surreptitiously configured computer servers under his control, including the Nagem Server, to route Internet traffic through the Ebury Botnet. The defendant configured the Nagem Server to route users who clicked on the link in the defendant's Spam e-mail messages through the Ebury Botnet to websites that had hired the defendant as an affiliate.

51. From on or about February 18, 2011, through the date of this Indictment, AFF paid tens of thousands of dollars to the defendant for his work as an affiliate, including by deposits into the "Mikhail Katsap" Payoneer account.

52. From on or about August 30, 2011, through the date of this Indictment, Infinity paid over one million dollars to the defendant for his work as an affiliate,

including by deposits into the defendant's "Stepan Demidov" Paxum account and by wire transfers to bank accounts held under the name "Germes Management, Ltd."

All in violation of Title 18, United States Code, Section 371.

COUNTS 2 - 3

(Violations of Computer Fraud and Abuse Act, 18 U.S.C. §§ 2 and 1030(a)(5)(A))

53. The allegations contained in paragraphs 1 – 16 and 19 – 52 of this Indictment are hereby realleged and incorporated by reference herein.

54. On or about the following dates, in the District of Minnesota and elsewhere, the defendant,

MAXIM SENAKH,
a/k/a "Mikhail Katsap,"
a/k/a "Andrey Rasputnikov,"
a/k/a "Stepan Demidov,"

knowingly caused the transmission of a program, information, code, and command, that is, malware, and, as a result of such conduct, intentionally caused damage and attempted to cause damage, without authorization, to a protected computer, thus causing damage affecting 10 or more protected computers during any one-year period, and causing loss aggregating at least $5,000 in value to one or more persons during any one-year period from a related course of conduct affecting one or more other protected computers, that is, administering and using the Ebury Botnet for click-fraud and Spam, all in violation of 18 U.S.C. §§ 2 and 1030(a)(5)(A), (c)(4)(A)(i)(I), (VI), (c)(4)(B):

Count Number	Computer	Date (on or about)
2	Minneapolis Server	August 26, 2013

3	Duluth Server	September 11, 2013

COUNTS 4 - 5

(Violations of Computer Fraud and Abuse Act, 18 U.S.C. §§ 2 and 1030(a)(2)(C))

55. The allegations contained in paragraphs 1 – 16 and 19 – 52 of this Indictment are hereby realleged and incorporated by reference herein.

56. On or about the following dates, in the District of Minnesota and elsewhere, the defendant,

MAXIM SENAKH,
a/k/a "Mikhail Katsap,"
a/k/a "Andrey Rasputnikov,"
a/k/a "Stepan Demidov,"

intentionally accessed the following computers without authorization, and exceeded authorized access, and thereby obtained information from a protected computer (namely, server log-on credentials), for purposes of commercial advantage and private financial gain, and in furtherance of any criminal and tortious act in violation of the Constitution and laws of the United States or of any state, all in violation of 18 U.S.C. §§ 2 and 1030(a)(2)(C), (c)(2)(B)(i) – (ii):

Count Number	Computer	Date (on or about)
4	Minneapolis Server	August 26, 2013
5	Duluth Server	September 11, 2013

COUNTS 6 - 7

(Violations of Computer Fraud and Abuse Act, 18 U.S.C. §§ 2 and 1030(a)(4))

57. The allegations contained in paragraphs 1 – 16 and 19 – 52 of this Indictment are hereby realleged and incorporated by reference herein.

58. On or before the following dates, in the District of Minnesota and elsewhere, the defendant,

MAXIM SENAKH,
a/k/a "Mikhail Katsap,"
a/k/a "Andrey Rasputnikov,"
a/k/a "Stepan Demidov,"

knowingly and with intent to defraud, accessed the following protected computers without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud, and obtained anything of value (namely, revenue from advertisers and server log-on credentials), all in violation of 18 U.S.C. §§ 2 and 1030(a)(4) and (c)(3)(A):

Count Number	Computer	Date (on or before)
6	Minneapolis Server	August 26, 2013
7	Duluth Server	September 11, 2013

COUNTS 8 - 11

(Wire Fraud, 18 U.S.C. §§ 2 and 1343)

59. The allegations contained in paragraphs 1 – 16 and 19 – 52 of this Indictment are hereby realleged and incorporated by reference herein.

60. On or about the following dates, in the District of Minnesota and elsewhere, the defendant,

MAXIM SENAKH,
a/k/a "Mikhail Katsap,"
a/k/a "Andrey Rasputnikov,"
a/k/a "Stepan Demidov,"

having devised and intending to devise a scheme and artifice to defraud Internet advertisers, and to obtain money and property (namely, revenue from click-fraud and Spam), by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, transmitted and caused to be transmitted, by means of the following wire communications, in interstate and foreign commerce, certain writings, signs, signals, pictures. and sounds, in violation of 18 U.S.C. §§ 2 and 1343:

Count Number	Description of Wire	Location of Wire	Date of Wire (on or about)
8	Install Ebury Malware on Minneapolis Server	To District of Minnesota	August 26, 2013
9	Transmit Stolen Credentials from Minneapolis Server	From District of Minnesota	August 26, 2013
10	Install Ebury Malware on Duluth Server	To District of Minnesota	September 11, 2013
11	Transmit Stolen Credentials from Duluth Server	From District of Minnesota	September 11, 2013

FORFEITURE ALLEGATIONS

61. Counts One through Eleven of this Indictment are hereby realleged and incorporated as if fully set forth herein by reference, for the purpose of alleging

forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B) and 1030(i), and Title 28, United States Code, Section 2461(c).

62. Upon conviction of any of Counts One through Eleven of this Indictment, the defendant shall forfeit to the United States any property, real or personal, constituting, or derived from, any proceeds obtained directly or indirectly as a result of such violations.

63. Upon conviction for any of Counts One through Seven of this Indictment, the defendant shall forfeit to the United States any person property that was used or intended to be used to commit or to facilitate the commission of such violations.

64. If any of the above-described forfeitable property is unavailable for forfeiture, the United States intends to seek the forfeiture of substitute property as provided for in Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), and by Title 28, United States Code, Section 2461(c).

65. All in violation of Title 18, United States Code, Sections 982(a)(2)(B); 1030(i); 371; 1030(a)(2)(C), (a)(4), and (a)(5)(A); and 1343.

A TRUE BILL

UNITED STATES ATTORNEY FOREPERSON